

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(национальный исследовательский университет)»**

**УТВЕРЖДЕНО**

**Проректор по учебной работе и  
довузовской подготовке**

**А.А. Воронов**

	<b>Рабочая программа дисциплины (модуля)</b>
<b>по дисциплине:</b>	Основы информационной безопасности
<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра управляющих и информационных систем
<b>курс:</b>	1
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Программу составил: В.А. Горбачев, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры управляющих и информационных систем 07.05.2020

## Аннотация

Дисциплина Основы информационной безопасности направлена на углубленное изучение современных задач, методов и средств защиты информации в компьютерных системах. В результате курса студенты ознакомятся с основными принципами обеспечения защиты информации, категориями мер защиты информации, принципами построения моделей угроз и нарушителей, а также оценки безопасности информационных технологий

### 1. Цели и задачи

#### Цель дисциплины

- ознакомление студентов с основами информационной безопасности: изучаются информационные угрозы, их нейтрализация, вопросы организации мер защиты информационных ресурсов, нормативные документы, регламентирующие информационную деятельность, криптография, другие вопросы, связанные с обеспечением информационной безопасности.

#### Задачи дисциплины

- изложить основные положения Доктрины информационной безопасности РФ;
- дать знания основ комплексной системы защиты информации;
- дать знания основ организационно-правового обеспечения защиты информации;
- сформировать основы для дальнейшего самостоятельного изучения вопросов обеспечения информационной безопасности.

### 2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области информатики и вычислительной техники, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.2 Способен оценивать актуальность исследований в области информатики и вычислительной техники и их практическую значимость
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов
	ОПК-4.2 Способен применять знание информационно-коммуникационных технологий для решения поставленной задачи, формулирования выводов и оценки полученных результатов
	ОПК-4.3 Способен аргументировано выбирать способ проведения научного исследования
	ОПК-4.4 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями

### 3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны знать:

содержание основных понятий обеспечения информационной безопасности;

источники угроз безопасности информации;

методы оценки уязвимости информации;

методы создания, организации и обеспечения функционирования систем комплексной защиты информации;

методы пресечения разглашения конфиденциальной информации;

виды и признаки компьютерных преступлений.

уметь:

отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

владеть:

методиками обеспечения информационной безопасности компьютерных систем

методиками анализа угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности.

#### **4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

##### **4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий**

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Информационные угрозы.	4			2
2	Компьютерные вирусы.	4			2
3	Правовое регулирование защиты информации (анализ статей УК, других нормативных актов).	4			2
4	Организационные меры обеспечения информационной безопасности компьютерных систем.	4			2
5	Защита данных криптографическими методами.	4			2
6	Политика информационной безопасности.	4			2
7	Типовые удаленные атаки с использованием уязвимостей сетевых протоколов.	6			3
Итого часов		30			15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

##### **4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)**

Семестр: 1 (Осенний)

###### **1. Информационные угрозы.**

Понятие информационных угроз. Понятие информации. Информационные войны. Изучаются основные определения информации, ее ценности, информационные угрозы. Информационные угрозы безопасности РФ. Доктрина информационной безопасности. Рассматриваются вопросы построения информационной структуры в РФ, различные проблемы, возникающие в связи с этим процессом, участие РФ в международном информационном обмене. Виды противников. Хакеры. Изучается социально-психологический портрет нарушителя информационной безопасности, его возможности и методика действий. Виды возможных нарушений информационной системы. Общая классификация информационных угроз. Изучаются нарушения работы ИС, вводится классификация угроз ИС, рассматриваются возможные субъекты и объекты доступа к ИС, угрозы, реализуемые на уровне локальной (изолированной) компьютерной системы. Причины уязвимостей компьютерных сетей.

## 2. Компьютерные вирусы.

Изучаются вредоносные программы, история их развития, ответственность за создание и распространение, виды, принципы действия вирусов, демаскирующие признаки.

## 3. Правовое регулирование защиты информации (анализ статей УК, других нормативных актов).

Стандарты ИБ. Нормативные документы, регулирующие информационную деятельность в РФ и мире. Стандарты информационной безопасности

## 4. Организационные меры обеспечения информационной безопасности компьютерных систем.

Роль задачи и обязанности администратора безопасности, определение подходов к управлению рисками, структуризация контрмер, порядок сертификации на соответствие стандартам в области ИБ

## 5. Защита данных криптографическими методами.

Методы и алгоритмы шифрования, требования к шифрам, наиболее распространенные шифры

## 6. Политика информационной безопасности.

Модели защиты информации в КС Политика безопасности и ее основные составляющие, модели защиты информации в компьютерных системах, технологии защиты и разграничения доступа к информации.

## 7. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов.

Классификация удаленных атак. Атаки на ARP- протокол, ICMP – протокол , DNS – протокол, TCP – протокол, виды атак.

# 5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная мультимедиа проектором, экраном и микрофоном.

## 6.Перечень рекомендуемой литературы

Основная литература

1. Расторгуев С. П. Основы информационной безопасности : учеб. пособие для студ. вузов, обуч. по спец. "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автомат. систем" и "Информ. безопасность телеком. систем"/ С. П. Расторгуев. -М.: Академия, 2007 .-192 с
2. Основы информационной безопасности : учеб. пособие для студ. вузов/ сост. Е. Б. Белов. -М.: Горячая линия - Телеком, 2006 .-544 с
3. В.Г. Олифер, Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы.-СПб.:Питер, 2001.- 672 с.
4. Ярочкин В.И. Информационная безопасность.- М.: Академический проект, 2003.-639 с.
5. Галатенко В.А. Основы информационной безопасности: Курс лекций.- М.: Интернет-Университет Информационных технологий, 2003. – 239 с.

Дополнительная литература

1. Федеральные законы РФ «О безопасности», «Об информации, информатизации и защите информации».
2. Федеральный закон РФ «О техническом регулировании».
3. Концепция национальной безопасности Российской Федерации.
4. Доктрина информационной безопасности Российской Федерации.
5. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовниченко и В.П. Шерстюка. -М., МЦНМО, 2002. -296с.
6. Коняевский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд», М., «Радио и связь», 1999, с 323.
7. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2001. -688 с.
8. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года.
9. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 года.
10. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года.
11. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года.
12. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение председателя Гостехкомиссии России от 30 марта 1992 года.
13. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 года.
14. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Решение председателя Гостехкомиссии России от 25 июля 1997 года.
15. Руководящий документ. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 год.
16. Руководящий документ. Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Гостехкомиссия России, 1999 год.
17. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Приказ председателя Гостехкомиссии России от 4 июня 1999 года № 114.
18. Руководящий документ. Безопасность информационных технологий, Критерии оценки безопасности информационных технологий. Часть 1, Часть 2, Часть 3. Приказ председателя Гостехкомиссии России от 19 июня 2002 года № 187.
19. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год.
20. Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 год.
21. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 год.
22. Руководящий документ. Безопасность информационных технологий. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год.
23. Стандарт МО США «Критерии оценки доверенных компьютерных систем» («Оранжевая книга»), 1983.

**7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

Не используются

**8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)**

не требуется

**9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций, так и интерактивных технологий, таких как собеседования, выполнение и обсуждение докладов и расчетных работ.

Подготовка и защита студентами докладов по темам, не входящим в план лекций, позволяет расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования, развить навык систематизировать и свободно излагать перед аудиторией материал по заданной теме.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

<b>по направлению:</b>	Информатика и вычислительная техника
<b>профиль подготовки:</b>	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра управляющих и информационных систем
<b>курс:</b>	<u>1</u>
<b>квалификация:</b>	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Дифференцированный зачет

**Разработчик:** В.А. Горбачев, канд. физ.-мат. наук, доцент



## 1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Имеет представление об актуальных проблемах науки и техники в области информатики и вычислительной техники, способен на научном языке формулировать профессиональные задачи	ОПК-2.1 Имеет представление о современном состоянии исследований в рамках тематической области своей профессиональной деятельности
	ОПК-2.2 Способен оценивать актуальность исследований в области информатики и вычислительной техники и их практическую значимость
	ОПК-2.3 Владеет профессиональной терминологией, используемой в современной научно-технической литературе, обладает навыками устного и письменного изложения результатов научной деятельности в рамках профессиональной коммуникации
ОПК-4 Способен успешно реализовывать решение поставленной задачи, провести анализ результата и представить выводы, применяя знания и навыки в области математики, естественных наук и информационно-коммуникационных технологий	ОПК-4.1 Способен применять знания и навыки по использованию информационно-коммуникационных технологий для поиска и изучения научной литературы, применения прикладных программных продуктов
	ОПК-4.2 Способен применять знание информационно-коммуникационных технологий для решения поставленной задачи, формулирования выводов и оценки полученных результатов
	ОПК-4.3 Способен аргументировано выбирать способ проведения научного исследования
	ОПК-4.4 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями

## 2. Показатели оценивания компетенций

В результате изучения дисциплины «Основы информационной безопасности» обучающийся должен:

### знать:

содержание основных понятий обеспечения информационной безопасности;  
источники угроз безопасности информации;  
методы оценки уязвимости информации;  
методы создания, организации и обеспечения функционирования систем комплексной защиты информации;  
методы пресечения разглашения конфиденциальной информации;  
виды и признаки компьютерных преступлений.

### уметь:

отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;  
применять действующую законодательную базу в области информационной безопасности;  
разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

### владеть:

методиками обеспечения информационной безопасности компьютерных систем  
методиками анализа угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности.

## 3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

#### 4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Перечень контрольных вопросов для дифференцированного зачета:

1. Сформулируйте понятие информации.
2. Что такое информационная безопасность?
3. Сравните понятия информационной безопасности и защиты информации.
4. Сформулируйте понятия доступности, целостности и конфиденциальности информации.
5. Что необходимо учитывать при анализе проблематики, связанной с информационной безопасностью?
6. Дайте определение понятий угроза, атака, уязвимость, злоумышленник.
7. По каким критериям классифицируются угрозы?
8. Охарактеризуйте наиболее распространенные угрозы доступности.
9. Что такое распределенная dos (ddos) атака на доступность?
10. Каковы грани вредоносного программного обеспечения?
11. Что такое вирусы и черви?
12. Что такое троянская программа?
13. Охарактеризуйте основные угрозы статической и динамической целостности.
14. Охарактеризуйте основные угрозы конфиденциальности.
15. Что такое перехват данных и маскард?
16. В чем заключаются меры законодательного уровня информационной безопасности?
17. Трактуйте преступлений в сфере компьютерной информации Уголовного кодекса РФ.
18. Дайте определение государственной тайны.
19. В чем заключаются принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации?
20. Каковы положения статьи 9 Закона "Об информации, информационных технологиях и о защите информации"?
21. Приведите основные определения, связанные с информацией, содержащиеся в Законе "Об информации, информационных технологиях и о защите информации".
22. Прокомментируйте положения статьи 16 Закона "Об информации, информационных технологиях и о защите информации".
23. Какие виды деятельности по обеспечению информационной безопасности подлежат лицензированию?
24. Раскройте понятия электронный документ, электронная цифровая подпись, Средства электронной цифровой подписи, ключи электронной цифровой подписи.
25. Сформулируйте цель Федерального закона "О Персональных данных" от 27 июля 2006 года.
26. Что такое персональные данные?
27. Раскройте содержание статьи 3 Федерального закона "О Персональных данных".
28. Сформулируйте принципы обработки персональных данных.
29. Проведите краткий обзор зарубежного законодательства в области информационной безопасности.
30. Сформулируйте следующие основные направления деятельности на законодательном уровне обеспечения ИБ.
31. В чем заключается сходство и различие оценочных стандартов и технических спецификаций?
32. Что такое «Оранжевая книга»?
33. Дайте определение доверенной системы, политики безопасности, уровня гарантированности в соответствии с «Оранжевой книгой».
34. Что такое монитор обращений в соответствии с «Оранжевой книгой»?
35. Охарактеризуйте механизмы безопасности в соответствии с «Оранжевой книгой».
36. Приведите основные классы безопасности в соответствии с «Оранжевой книгой».
37. Охарактеризуйте сервисы безопасности и исполняемые ими роли в соответствии с Рекомендациями X.800.
38. Что такое администрирование средств безопасности в соответствии с Рекомендациями X.800?

39. Что содержат Общекритерии оценки безопасности информационных технологий?
40. Каковы основные требования Общих критериев?
41. Какова иерархия пространства требований Общих критериев?
42. Раскройте понятия Профиль защиты и Задание по безопасности".
43. Сформулируйте классы функциональных требований Общих критериев.
44. Проанализируйте требования доверия безопасности Общих критериев.
45. Охарактеризуйте Гармонизированные критерии ИБ Европейских стран.
46. Проведите классификацию ФСТЭК(Гостехкомиссии РФ) автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД).
47. Проведите классификацию ФСТЭК (Гостехкомиссии РФ) межсетевых экранов.
48. В чем заключается цель административного уровня обеспечения ИБ?
49. Что такое политика безопасности?
50. Каковы уровни политики безопасности?
51. Что такое программа безопасности?
52. Каковы этапы жизненного цикла автоматизированной системы?
53. Как осуществляется синхронизация программы безопасности с жизненным циклом автоматизированных систем?
54. Что такое управление информационными рисками?
55. Какие действия возможны по отношению к выявленным рискам?
56. Каковы этапы процесса управления информационными рисками?
57. Как осуществляется выбор анализируемых объектов и уровня детализации их рассмотрения?
58. Как связан процесс управления рисками с жизненным циклом АС?
59. В чем заключается идентификация активов и угроз в процессе управления рисками?
60. Как осуществляется оценка вероятности осуществления угрозы?
61. Какие шкалы используются для оценки рисков?
62. Как оценивается стоимость мер защиты?
63. Каковы классы мер процедурного уровня обеспечения ИБ?
64. Поясните принципы минимизации привилегий и разделения обязанностей при управлении персоналом.
65. В чем заключается основной принцип физической защиты информации?
66. Каковы направления физической защиты информации?
67. В чем заключается смысл декомпозиции контролируемой территории
68. Охарактеризуйте мероприятия, направленные на поддержание работоспособности АС.
69. Что включает в себя инфраструктура АС?
70. Что такое информационная избыточность?
71. Поясните важность программно-технических мер защиты информации.
72. На какие виды можно разделить меры информационной безопасности?
73. В чем заключаются особенности современных АС, существенные с точки зрения ИБ?
74. Что такое монитор обращений сетевой конфигурации?
75. В чем заключаются принципы архитектурной безопасности АС?
76. Поясните смысл принципа непрерывности защиты.
77. Поясните смысл принципа эшелонированности защиты.
78. Поясните смысл принципа минимизации объема защитных средств, выносимых на клиентские системы.
79. Поясните различие между процессами идентификации и аутентификации.
80. В чем достоинства и недостатки парольной аутентификации?
81. В чем заключаются меры повышения надежности парольной защиты?
82. Что такое одноразовый пароль и каковы его особенности?
83. Что такое сервер аутентификации?
84. Какие задачи решает протокол Kerberos?
85. Что такое биометрия?
86. Что такое биометрический шаблон?
87. Поясните понятие матрицы доступа.
88. В чем заключаются различия между дискреционным и мандатным методами доступа?
89. В чем суть ролевого метода управления доступом?

90. Раскройте понятия ролевого управления доступом.
91. Раскройте смысл статического и динамического распределения обязанностей при ролевом управлении доступом.
92. Что такое протоколирование?
93. Что такое аудит?
94. Какие задачи решает реализация протоколирования и аудита?
95. Дайте определение сигнатуры атаки.
96. Как выявляется подозрительная активность пользователя?
97. Какие имеются средства активного аудита?
98. Какие методы шифрования являются основными?
99. Приведите схемы симметричного и асимметричного шифрования.
100. Поясните понятие Хэш - функции.
101. Приведите схему выработки электронной цифровой подписи (ЭЦП).
102. Что такое удостоверяющий центр и цифровой сертификат?

Примеры билетов:

Билет №1

1. Сформулируйте принципы обработки персональных данных.
2. Что такое аудит?

Билет №2

1. Что такое перехват данных и маскаррад?
2. Дайте определение сигнатуры атаки.

#### Критерии оценивания

Оценка отлично (10) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (9) выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично (8) выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо (7) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо (6) выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Оценка хорошо (5) выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно (4) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно (3) выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых

понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно (2) выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно (1) выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

## **5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Дифференцированный зачет проводится в устной форме.

При проведении дифференцированного зачета обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося по билету на зачете не должен превышать двух астрономических часов.

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины и конспектами лекций.